Deloitte.

The Aftermath of Schrems II

Implications, insights, and expectations for the future.

November 2022

MAKING AN IMPACT THAT MATTERS since 1845

Table of contents

Introduction

In June 2020, the Court of Justice of the European Union (**CJEU**) invalidated the legal basis for data transfers from the European Union (**EU**) to the United States in its Schrems II judgment. This decision has significant implications for organizations around the world. Almost two years post-Schrems II, this paper discusses the implications of the judgment and looks at the current data transfer landscape.

First, a brief recap of the road leading up to Schrems II is provided, followed by an overview of the conclusions reached in the case. Second, the response to Schrems II – both in terms of legislation and enforcement – is discussed in light of selected decisions by national Data Protection Authorities (**DPAs**) as well as the European Data Protection Supervisor (**EDPS**). Lastly, currently pending developments and the future of international data transfers are considered.

Schrems in a nutshell

The EU General Data Protection Regulation (**GDPR**) states that any transfer of personal data to a third country is conditional upon an adequate level of data protection being provided in the third country concerned.[1] This requirement is the main point of contention in relation to EU-US data transfers. EU-US data flow arrangements have been the subject of much attention, starting with the Safe Harbour Agreement of July 2000 between the US Department of Commerce and the European Union. This agreement was invalidated by the CJEU in 2015, in the Schrems I ruling. Thereafter, the EU-US Privacy Shield was designed and adopted to provide a (so-called) adequate level of data protection to trans-Atlantic data transfers and to ensure consistency with EU data protection legislation in the transfer of EU citizens' personal data to the US.[2] However, the EU-US Privacy Shield still left room for indiscriminate access to personal data in the name of national security in the US, which led to its eventual invalidation in 2020 (well known as the Schrems II ruling).

With EU-US Privacy Shield gone, data controllers are left to rely on other mechanisms for EU-US data transfers, such as Standard Contractual Clauses (**SCCs**). Although the CJEU upheld the validity of SCCs in Schrems II, the CJEU noted that data controllers must ensure that "*data subjects … are afforded a level of protection essentially equivalent to that guaranteed within the European Union by [the GDPR] (…) – where necessary [with] additional safeguards to those offered by those clauses.*"[3] The CJEU also held that where controllers failed to meet these requirements, data transfers must be suspended. DPAs must check and prohibit data transfers where data subjects are not afforded such a level of data protection.

[1] Art. 44, 45 GDPR.

[2] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield; https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf (consulted on 3 June 2022).

[3] Case C-311/18 (2020), *Data Protection Commissioner v. Facebook Ireland Ltd. (Schrems II)*, par. 105, 134; https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf, p. 2 (consulted on 3 June 2022).

Post Schrems II

Legislative guidance to navigate Schrems II

In the wake of the Schrems II judgment, many European organizations and national DPAs were uncertain about how to ensure the compatibility of international data transfers with the GDPR. Not only was the EU-US Privacy Shield invalidated, but SCCs could no longer automatically be relied upon either. As previously mentioned, the CJEU imposed an additional requirement on organizations to perform a case-by-case transfer impact assessment to determine if additional safeguards are needed to comply with the GDPR.[4]

In an attempt to mitigate post-Schrems II confusion and provide guidance, the European Data Protection Board (**EDPB**) published a set of recommendations in June 2021 (**Recommendations**).[5] The European Commission also updated the standard SCCs.[6] The updated SCCs, specifically clause 14, should be read in conjunction with the Recommendations. Clause 14 requires parties engaged in international data transfers to ensure, prior to concluding the SCC, that the recipient jurisdiction offers an equivalent level of data protection as is mandated in the EU. This assessment of the level of data protection in the recipient jurisdiction is known as a "Transfer Impact Assessment" (**TIA**).[7] The Recommendations set out the steps to conduct such a TIA. It also contains a list of possible information sources for the TIA, as well as examples of supplementary measures. If the results of the TIA are insufficient, extra safeguards must be put in place by the parties in order to be able to conclude the SCC.[8] The updated SCCs came into force on September 27, 2021 and have had to be used for new data transfer contracts since that date. The final compliance deadline for pre-Schrems II contracts to transition to the new SSCs and comply with the Schrems II requirements is on December 27, 2022.

In addition to legal supplementary measures, technical measures may also function as effective additional safeguards in international data transfers. A widely known example is the use of encryption, which can be especially effective where a neutral third party holds the decryption key. However, technical measures such as encryption, data pseudonymization, and split- or multi-party processing often raise practical and functional issues.[9] End-to-end encryption, for example, often results in a reduction in functionality and features.[10] Pseudonymization involves similar limitations and creates a risk of re-identification of data.[11]

[4] Case C-311/18 (2020), *Data Protection Commissioner v. Facebook Ireland Ltd. (Schrems II)*, par. 134; https://www2.deloitte.com/bg/en/pages/about-deloitte/articles/new-challenges-in-personal-data-transfers.html (consulted on 3 June 2022).
[5] https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (consulted on 3 June 2022).
[6] Annex to the Commission Implementing decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, C(2021) 3972; https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/risk/lu-rna-european-commission-standard-contractual-clauses.pdf (consulted on 3 June 2022); https://www2.deloitte.com/dl/en/pages/legal/articles/standardvertragsklauseln-internationaler-datentransfer.html (consulted on 3 June 2022).
[7] Annex to the Commission Implementing decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, C(2021) 3972, Clause 14.
[8] The new Standard Contractual Clauses – Questions and Answers, p.22. https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf); https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=EN (consulted on 3 June 2022).
[9] https://iapp.org/news/a/uncertainty-aplenty-a-year-after-schrems-ii-ruling/; https://www.forbes.com/sites/forbestechcouncil/2022/04/14/the-rise-of-encryption-in-a-schrems-ii-world/; https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, p.30-34 (consulted on 3 June 2022).
[10] https://www.forbes.com/sites/forbestechcouncil/2022/04/14/the-rise-of-encryption-in-a-schrems-ii-world/ (consulted on 3 June 2022).
[11] https://www.itgovernance.co.uk/blog/the-gdpr-requirements-for-encryption (consulted on 29 May 2022).

Territorial solutions, namely the storing of data on EU soil rather than outside the EU, have also been considered. Microsoft, for example, is committed to enabling organizations to store and process data within the EU through their "EU Data Boundary for Microsoft Cloud" plan.[12] However, this is not a solution for all organizations. Especially smaller organizations may not have the resources to do this.[13] Moreover, the French DPA recognized that localization of personal data in the EU may still be subject to impact/risk assessments and subsequent additional safeguards, especially where the organizations hosting the data are subject to a foreign jurisdiction.[14]

[12] https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/ (consulted on 3 June 2022).
[13] https://www.forbes.com/sites/forbestechcouncil/2021/02/17/data-privacy-day-heres-what-the-eus-schrems-ii-decision-means-for-us-companies/ (consulted on 3 June 2022).
[14] Conseil d'Etat, Amazon case; https://www.lawyerpress.com/wordpress/wp-content/uploads/2022/01/Data-Breach-Report-2022_DLAPIPER.pdf (consulted on 3 June 2022).

Enforcing Schrems II

While the EDPB and the European Commission have provided some guidance on the execution of post-Schrems II international data transfers, decisions reached by national DPAs as well as by the European Data Protection Supervisors (**EDPS**) also offer valuable insights into what can be expected when it comes to the enforcement of Schrems II. A few decisions, particularly their relevance and implications, are briefly discussed below.

Various DPAs decisions on requiring TIAs per Schrems II

The earliest decisions on the enforcement of Schrems II by national DPAs primarily concerned the new TIA requirement that followed the judgment.

One of the first decisions relating to TIAs was issued by the DPA of the German state of Bavaria in March 2021. In this decision, the Bavarian DPA established that data transfers from a German company to Mailchimp (US based) were illegal because the German company had not performed a TIA to assess whether additional measures were needed to supplement the SCC facilitating the transfer. According to the Bavarian DPA, such an assessment was necessary because there were indications that MailChimp may be subjected to data access by US surveillance services.[15]

In the same month, the French Conseil d'État in cooperation with the French DPA ruled on a complaint concerning the safeguards against US authorities' access to data held by a Luxemburg-based subsidiary of Amazon Web Services, AWS Sarl, for covid testing provider Doctolib. The data concerned was hosted by AWS Sarl centers in France and Germany. Moreover, the contract between Doctolib and AWS Sarl explicitly prevented data transfers to the US. As mentioned, AWS Sarl is a subsidiary of Amazon Web Services, a company subject to U.S. jurisdiction. Therefore, AWS Sarl may become subject to access requests by the US authorities. However, the Court concluded that while there is a risk of such access requests, the legal and technical safeguards in place were sufficient to protect the data involved. This decision is significant as the Court recognized that even where *in principle* no data transfers to third countries occur and data is stored on EU soil, it can still be subject to access requests by US authorities using extra-territorial US laws.[16] The ruling also indicates that storing data locally on EU territory does not remove it from the scrutiny of Schrems II – specifically when the data hosted is on European territory by subsidiaries of non-EU organizations that may be subject to foreign jurisdictions.[17]

In April 2021, the Portuguese DPA issued a decision ordering the suspension of international data transfers from the National Institute of Statistics using Cloudflare based. The decision was based on the inadequacy of the TIA conducted by the National Institute of Statistics, and the subsequent insufficient safeguards that accompanied the SCCs in question. In its assessment, the National Institute for Statistics focused solely on security but failed to assess broader risks. Moreover, the data processing agreement stated that Cloudflare would notify the National Institute of Statistics of government requests into the data, but only if it was not prohibited from doing so. As this is often the case with regard to national security activities, it was determined that this provision did not provide sufficient protection. Based on this, the Portuguese DPA ordered the suspension of data transfers within 12 hours. This case is relevant and differs from previous decisions, as it concerns the actual substance of assessments and safeguards.[18]

[15] https://edpb.europa.eu/news/national-news/2021/bavarian-dpa-baylda-calls-german-company-cease-use-mailchimp-tool_en **(consulted on 3 June 2022).**
[16] https://medium.com/protectionofdata/doctolib-ruling-does-schrems-ii-now-apply-to-inter-eu-transfers-feda0e987779 (consulted on 7 June 2022).
[18] https://www.allenovery.com/en-gb/global/blogs/digital-hub/schrems-ii-portuguese-dpa-suspends-data-transfer-to-the-us-by-public-entity-that-relied-on-standard-contractual-clauses; https://edpb.europa.eu/news/national-news/2021/census-2021-portuguese-dpa-cnpd-suspended-data-flows-usa_en; https://iapp.org/news/a/schrems-ii-dpa-investigations-and-enforcement-lessons-learned/ **(consulted on 29 May 2022).**
[18] https://www.allenovery.com/en-gb/global/blogs/digital-hub/schrems-ii-portuguese-dpa-suspends-data-transfer-to-the-us-by-public-entity-that-relied-on-standard-contractual-clauses; https://edpb.europa.eu/news/national-news/2021/census-2021-portuguese-dpa-cnpd-suspended-data-flows-usa_en; https://iapp.org/news/a/schrems-ii-dpa-investigations-and-enforcement-lessons-learned/ **(consulted on 29 May 2022).**

Austrian DPA decision on the use of Google Analytics violating Schrems II

The Austrian DPA ruled on one of the model cases filed by Noyb (a not-for-profit organization initiated by Max Schrems and focused on privacy and data protection issues) in January 2022, concerning the use of Google Analytics by an Austrian website. The Noyb filed 101 such model cases, concerning identical complaints against European organizations that continue to provide data about their website visitors to Google and Facebook. The complaints seek to address whether transfers of EU personal data to Google and Facebook in the US through the use of cookies is still permitted in light of the Schrems II ruling. The decision of the Austrian DPA established that the use of Google Analytics by an Austrian website, through which personal data was transferred to Google LLC in the US, violated Chapter V of the GDPR and the conclusions reached in Schrems II. The safeguards encapsulated in the SCC were deemed insufficient to protect the data from access by US intelligence services. Additionally, Google LLC had implemented contractual and organizational supplementary measures. These measures included carefully considering any data requests, notifying data subjects about data requests, and publishing transparency reports and guidelines for handling government requests. Technical supplementary measures were also implemented, such as protection of communications between Google services and between users and websites, protection of data in transit between data centers, onsite security, encryption technologies, and pseudonymization. However, these contractual, organizational and technical supplementary measures were not considered sufficient. The DPA considered that it was not apparent to what extent these supplementary measures are effective to close the gap in data protection levels between the EU and the US. Further, the Schrems II ruling recognized that even permissible (i.e. legal under US law) requests from US intelligence agencies are incompatible with the fundamental right to data protection under Article 8 of the EU Charter of Fundamental Rights.[19] Therefore, the Austrian DPA ruled that the data transfer taking place, in this case, constituted a violation of the GDPR and Schrems II.[20]

Google Analytics is one of the most widely used statistics programs that many organizations and websites rely on and use. Therefore, this decision of the Austrian DPA is one of the most impactful decisions since the Schrems II judgment itself.[21] The complaint handled in this case constituted merely one of the 101 complaints filed by Noyb, and will likely open the floodgates for similar decisions on the remaining complaints. This has also become apparent from statements made by other DPAs, notably the Danish and Norwegian authorities. The Norwegian DPA stated that it is dealing with two similar cases concerning the use of Google Analytics and that its decision will be "influenced by European practice on this topic"[22]. The Norwegian DPA also advised organizations to examine the use of alternative programs to Google Analytics. The Danish DPA explicitly recognized the importance of a consistent interpretation of data privacy rules among European national DPAs. Similar to the Norwegian DPA, the Danish DPA also confirmed that it will base its decisions regarding the use of Google Analytics on the ruling of the Austrian DPA and other upcoming decisions on this topic.[23]

[19] https://fpf.org/blog/understanding-why-the-first-pieces-fell-in-the-transatlantic-transfers-domino/ (consulted on 3 June 2022).
[20] https://www.orrick.com/en/Insights/2022/02/The-Austrian-Data-Protection-Authority-Groundbreaking-Google-Analytics-Decision (consulted on 3 June 2022).
[21] https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal (consulted on 3 June 2022).
[22] https://www.orrick.com/en/Insights/2022/02/The-Austrian-Data-Protection-Authority-Groundbreaking-Google-Analytics-Decision; https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/google-analytics-kan-vare-ulovlig/?mkt_tok=MTM4LUVaTS0wNDIAAAGCPhVhupy_fJZqD9SImxn4-l1KSBMYDD64tSn0ZXXGPkBbp-hStsOl91WjXl_0pEK8xfWZtnKwCMAOHiFlEA-qi0l2FhzE4XxouoC6vCM4fAaG (consulted on 3 June 2022).
[23] https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal; https://www.orrick.com/en/Insights/2022/02/The-Austrian-Data-Protection-Authority-Groundbreaking-Google-Analytics-Decision; https://noyb.eu/en/austrian-dsb-eu-us-data-transfers-google-analytics-illegal (consulted on 7 June 2022).

EDPS decision on violation of Schrems II by European Parliament

In October 2020, the EDPS received one of the first complaints against the European Parliament following the Schrems II judgment. The EDPS is the European Union's independent data protection authority. The EDPS monitors and ensures the protection of personal data and privacy when European institutions and bodies process the personal data of individuals. Further, the EDPS advises the European bodies with regard to the processing of personal data. The rules regarding data protection obligations for the EU institutions are enshrined in Regulation (EU) 2018/1725, which is essentially equivalent to the GDPR.[24] The regulation was instated to ensure that *"the EU institutions and bodies … as well as the EDPS itself, are now subject to the same rigor as controllers under the GDPR"*[25]. This Regulation is often described as the "public sector counterpart" of the GDPR.[26] EDPS also cooperates with national DPAs to improve consistency and coherence in the landscape of personal data protection. The EDPS is headed by a Supervisor, who is supported by a secretariat of lawyers, IT specialists, and administrators.[27]

The complaint brought before the EDPS concerned the internal covid testing website of the Parliament, which allegedly violated Article 15 and Chapter V of Regulation (EU) 2018/1725 on grounds of confusing cookie banners, unclear data protection notices, and illegal data transfers to the US.[28] The EDPS found that personal data of visitors of the Parliament's aforementioned website was processed and transferred to the US, as a result of the placement of tracking cookies from US-based companies (such as payment processing software company Stripe and Google Analytics) on the website concerned.

The EDPS stated that "*the Parliament provided no documentation, evidence or other information regarding the contractual, technical or organizational measures in place to ensure an essentially equivalent level of protection to the personal data transferred to the US in the context of the use of cookies on the website.*"[29] Accordingly, in January 2022 the EDPS concluded that that the website's use of Google Analytics and the payment provider Stripe violated the Schrems II ruling. While no fine was imposed, the EDPS issued a reprimand against the Parliament for various violations of Regulation (EU) 2018/1725 and a time limit of one month to update the data protection notice and remaining issues on its covid testing website.[30]

[24] https://edps.europa.eu/sites/edp/files/publication/ar2018_en.pdf, p. 9 **(consulted on 3 June 2022).**
[25] https://edps.europa.eu/sites/edp/files/publication/ar2018_en.pdf, foreword **(consulted on 3 June 2022).**
[26] https://www2.deloitte.com/content/dam/Deloitte/be/Documents/risk/2019-Deloitte-GDPR-for-European-Union-Institutions-Viewpoint.pdf **(consulted on 3 June 2022).**
[27] https://edps.europa.eu/about-edps_en **(consulted on 3 June 2022).**
[28] Decision of the European Data Protection Supervisor in complaint case 2020-1013, submitted by Members of the Parliament against the European Parliament (https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf_); https://noyb.eu/en/edps-sanctions-parliament-over-eu-us-data-transfers-google-and-stripe **(consulted on 3 June 2022).**
[29] https://noyb.eu/sites/default/files/2022-01/Case%202020-1013%20-%20EDPS%20Decision_bk.pdf, p. 14 **(consulted on 3 June 2022).**
[30] https://noyb.eu/en/edps-sanctions-parliament-over-eu-us-data-transfers-google-and-stripe **(consulted on 3 June 2022).**

What is to come – a possible Schrems III?

While legislative guidance and enforcement by DPAs have helped provide insight into the scope of the Schrems II ruling and its implications for future EU-US data transfers, there is still more to come. On March 25, 2022, the European Commission and the US government announced the new 'Trans-Atlantic Data Privacy Framework', intended to foster trans-Atlantic data flows and address the concerns raised by the CJEU in Schrems II.[31]

The Trans-Atlantic Data Privacy Framework is currently an 'agreement in principle' and is yet to be translated into legal documents. The principal objective of this new framework is to curb data access by US intelligence agencies and to enable data to flow freely and safely between the US and participating US organizations. The new framework aims to introduce a new set of rules and binding safeguards that limit access to data by US intelligence agencies based on necessity and proportionality. [32] To ensure this, procedures shall be established and adopted by US intelligence agencies to ensure effective oversight of new standards for privacy and civil liberties. Further, a two-tier redress system and a Data Protection Review Court are envisaged in order to investigate and resolve complaints of Europeans on data access by US intelligence authorities.[33] The new framework shall also put forth strong obligations for organizations processing the personal data of European citizens. These obligations include specific monitoring and review mechanisms, as well as a self-certification requirement indicating adherence to the principles of the new framework through the US Department of Commerce.

The principles and safeguards that will be included in Trans-Atlantic Data Privacy Framework could potentially solve the problems surrounding EU-US data transfers. But this brings to attention a fundamental question – why have the Trans-Atlantic Data Privacy Framework in the first place? The significance and volume of data transfers between the EU and the US are evidently tremendous, as many big tech companies are based in the US. With such business being a priority, it seems sensible to have a framework to simplify EU-US data transfers. However, given the history of two such frameworks (i.e. Safe Harbour Agreement and Privacy Shield) being annulled by the CJEU, can organizations trust that the Trans-Atlantic Data Privacy Framework will deliver on its promises and fill the gaps of its predecessors? There always remains the risk that the Trans-Atlantic Data Privacy Framework (as well as any other potential framework for data transfers to a third country) could be brought to question before the CJEU, and potentially be considered an inadequate data transfer mechanism. This risk seems all the more likely, as was recognized by Noyb in May 2022 in an open letter on the future of EU-US data transfers. Noyb warned that "*the announced framework risks sharing the same fate as its two predecessors in front of the CJEU unless substantive (legislative) reforms are conducted in the United States*".[34]

[31] https://ec.europa.eu/commission/presscorner/detail/es/ip_22_2087 (consulted on 3 June 2022).
[32] Transatlantic Data Privacy Framework, European Commission, March 2022, available at https://ec.europa.eu/commission/presscorner/detail/en/FS_22_2100 (consulted on 3 June 2022).
[33] Id.
[34] https://noyb.eu/en/open-letter-future-eu-us-data-transfers (consulted on 7 June 2022).

Ultimately, it might be safer for organizations to rely on other mechanisms for data transfers as a long-term solution. For these reasons, it is important to further strengthen SCCs as a valid data transfer mechanism by ensuring that parties are able to self-regulate and undertake to provide an adequate level of protection for data transfers. However, the requirement for organizations to undertake TIAs for data transfers to essentially all third countries comes with many challenges – organizations must ensure they have the right expertise on local laws, which can be cumbersome if organizations do not have data privacy experts at hand. Conducting TIAs also requires a reasonable budget and needs to be accounted for in the financial planning of the organization. While it is recommended that organizations conduct and document a TIA for every international data transfer to ascertain that data importers actually fulfill the obligations in the new SCCs, this may be difficult in practice. Organizations may have to prioritize TIAs for certain data transfers over others considering the availability of budget as well as expertise. Ultimately, the risk appetite of the organization is an important factor to consider as well.

Our experience

Deloitte's Cyber Privacy and Digital Ethics team has experience in supporting our clients in dealing with challenges relating to international transfers. For example, we help our clients to identify data transfer risks and assist them in strategizing and operationalizing appropriate and effective responses to mitigate these risks. We see that organizations must balance their resources and time allocation between what is needed to address these risks and other relevant priorities. New obligations such as conducting TIAs come on top of already existing obligations (such as SCCs, data privacy impact assessments, or privacy by design assessments). Our privacy professionals support our clients in approaching this in a streamlined and effective manner, building on and creating synergies.

Identifying the landscape of data transfers in an organization requires the involvement of multiple stakeholders and a thorough understanding of the business processes involved. The concept of a data transfer is substantially broad and can thus have a significant impact on third-party relationships. Organizations may find that their record of processing activities or current asset inventories require additional details to reliably identify data transfers or destination countries. At the same time, efforts to map out this information already exist in most organizations. Enhanced efforts needed for data transfer identification generally improve overall accountability and transparency.

In our experience, it is effective to utilize a workable and structured approach to (amongst other things) identify the scope of transfers, set up categorizations of data, and determine safeguards per category. Our experts are qualified in finding pragmatic solutions for data transfer risks that match the organization's processes and way of working.

Conclusion

(Legal) uncertainty surrounding Schrems II persists despite various efforts to clarify and guide such transfers. The Trans-Atlantic Data Privacy Framework might bring some direction and certainty with regard to EU-US data transfers. However, the future of the announced framework remains dubious and data transfers to other third countries remain untouched by this mechanism. This calls for further development of measures facilitating safe international data transfers. Using our strategies and expertise, we help our clients with navigating international data transfers. For more information, please contact Annika Sponselee, Partner in Risk Advisory and Global Data & Privacy Lead of Deloitte.

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities (collectively, the "Deloitte organization"). DTTL (also referred to as "Deloitte Global") and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the "Deloitte organization") serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 312,000 people make an impact that matters at www.deloitte.com.